Màster en Relacions Internacionals Seguretat i Desenvolupament (MURISD)

NATO's Response to Hybrid Warfare and Threats: State and non-State Actors

Autora: Stefania Mascolo

Tutor: Juan Pablo Soriano

Treballs de màster i postgrau. Màster en Relacions Internacionals, Seguretat i Desenvolupament (MURISD). Curs 2017/18

Universitat Autònoma de Barcelona

Treballs de màster i postgrau. Màster en Relacions Internacionals, Seguretat i desenvolupament (MURISD). Curs 2017/18

http://murisd.uab.cat

Coordinador de la col·lecció: Dr. Rafael Grasa Hernández, Rafael.Grasa@uab.cat.

Aquesta col·lecció recull una selecció de treballs duts a terme pels estudiants del Màster Universitari en Relacions Internacionals, Seguretat i Desenvolpament. Els treballs es publiquen en algunes de les tres llengües del màster, català, castellà i anglès

Esta colección recoge una selección de trabajos realizados por estudiantes del Máster Universitario en Relaciones Internacionales, Seguridad y Desarrollo. Los trabajos se publican en algunas de las tres lenguas del máster, catalán, castellano y inglés

This collection includes a selection of research by students of Master's Degree in International Relations, Security and Development. These researches are published in any of the three languages of the master's degree, catalan, spanish and english

Universitat Autònoma de Barcelona

MÁSTER UNIVERSITARIO EN RELACIONES INTERNACIONALES, SEGURIDAD Y DESARROLLO

NATO's Response to Hybrid Warfare and Threats: State and non-State Actors

Stefania Mascolo

Tutor Juan Pablo Soriano

Convocatoria

Septiembre 2018

Número total de palabras: 12030

Declaro, con mi firma al pie, que el presente trabajo es original y que no contiene plagios o usos indebidos de otras fuentes y acepto las consecuencias que podría tener contravenir el presente compromiso.

Firma

Stefania Mascolo

Summary

This paper intends to give an overview of the current position of the North Atlantic Treaty Organization (NATO) in the international security context, identifying NATO's perspective and response on one of the main security threats: the rising of hybrid warfare tactics performed by State and non-State actors (NSA). It deepens the hybrid warfare concept, as defined by major expert Frank Hoffmann, as academic-technical word, and its actual importance on NATO's strategic and operational course of action. An evaluation on NATO's tools will lead to synthetic and punctual recommendations for the Organization, experts and policy-makers to implement and improve NATO's capabilities

Aquest document pretén donar una visió general de la posició actual de l'Organització del Tractat de l'Atlàntic Nord (OTAN) en el context de la seguretat internacional, identificant la perspectiva i la resposta de l'OTAN en una de les principals amenaces de seguretat: l'augment de les tàctiques de guerra híbrides realitzades per l'Estat i no Actors d'estat (NSA). Enfoca el concepte de guerra híbrida, tal com el defineix l'expert principal Frank Hoffmann, com a paraula acadèmica-tècnica, i la seva importància real sobre el curs d'actuació estratègica i operativa de l'OTAN. Una avaluació sobre les eines de l'OTAN donarà lloc a recomanacions sintètiques i puntuals per a l'Organització, els experts i els responsables polítics per implementar i millorar les capacitats de l'OTAN.

Key Words

International security, Western Defence, NATO, Hybrid Warfare.

Seguretat internacional, Defensa occidental, OTAN, Guerra híbrida.

Contents

Executive Summary

This paper intends to give an overview of the current position of the North Atlantic Treaty Organization (NATO) in the international security context, identifying NATO's perspective and response on one of the main security threats: the rising of hybrid warfare tactics performed by State and non-State actors (NSA).

Adopting major expert Frank Hoffmann's definition of hybrid warfare as a complex coordination of conventional and non-conventional military capabilities, including political, economic, diplomatic means, including terrorism, organized crime, cyberattacks, as elements operating coherently and simultaneously, creating a powerful synergic effect.

This policy paper deepens the hybrid warfare topic as academic-technical word, created in a Western-centered perspective, how much true or new is the concept and the actual importance that the debate on the existence of a new warfare does have on NATO's strategic and operational action.

As unstructured form of war, hybrid warfare is not only mastered by non-state actors, but also by states.

NATO as political-military organization born in a context of traditional military state-security threats, is now facing blurred threats and multi-shape enemies, highly interconnected and constantly evolving. To do not get obsolete, NATO needs to reinvent itself, updating its perspective and tools beyond the military approach and embracing a multi-dimensional nature that can effectively guarantee peace and security for the Alliance.

The analysis touches upon interaction among the different levels of the international system: a supra national level, represented by NATO, a state-one like Russia and transnational like terrorist groups. Considering the crisis that sovereign states are living, they are increasingly not able to face alone global security issues, which are also more and more interconnected and cross-border, fact that foster, or should do, a stronger cooperation among states and therefore, stimulating a supranational level of action.

NATO represents a strong forum of dialogue, cooperation and action in this troubled moment for the West, but often different interests and opinions among the Allies slow down or block a powerful unified response to current and future challenges.

As cases of study, Russia, considered one of the few states which employ effectively hybrid warfare, as demonstrated in the Ukraine crisis and the chaos created by the so-called Gerasimov Doctrine. In the Middle East, private groups successfully use hybrid warfare to overcome their military weakness, bypassing international law, gaining international status. These two actors are the emblematic examples of the entrance of the international security environment into a hybrid era.

List of Acronyms

ACO	Allied Command of Operations
DAT	Defence e Against Terrorism
EU	European Union
FOI	Swedish Defence Research Agency
IDF	Israeli Defence Forces
ISIS	Islamic State of Iraq and Syria
NATO	North Atlantic Treaty Organization
NFIU	NATO Force Integration Units
NRF	NATO Response Force
NSA	Non-state Actors
NSAG	Non-state Armed Groups
NSHQ	NATO Special Operations Headquarters
PAP – T	Partnership Action Plan against Terrorism
POW	Program of Work
RAP	Readiness Action Plan
RMA	Revolution in Military Affairs
SHAPE	Supreme Headquarters Allied Powers Europe
SOF	Special Operations Forces
UN	United Nations
URSS	Union of Soviet Socialist Republics
US	United States of America
VJTF	Very High Readiness Joint Task Force

"Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after changes occur."

Italian air-power theorist Giulio Douhet. 1921.

1. Introduction

As policy paper is structured in three main chapter, an introductive chapter about the current security environment, an inside look in NATO's response chapter, divided in strategic and operational part, and a third chapter dealing with cases of studies, i.e. Russia and terrorism in the Middle East as significative example of state and non-state actors engaging hybrid warfare and representing a threat to the Alliance.

Particularly significant is the NATO's response chapter, in which NATO strategy is analysed in two main aspects: its theorical conceptualization, i.e. NATO coherent vision and perspective shape its comprehension and reaction to hybrid threats, and its operational response, i.e. NATO concretization of the previous developed strategy, through concrete military tools and operations.

The main objective of the analysis is the study of NATO, The North Atlantic Treaty Organization, in its approach to hybrid warfare, as defined by Frank G. Hoffman in "Hybrid Warfare and Challenges". The hybrid warfare is an unstructured form of war, used by States, as demonstrate by the high Russian capability, and mastered by non-State actors. The Middle East has seen the rise of terrorist groups winning against state military forces thanks to the successful use of hybrid warfare, as shown by Hezbollah group in the 2007 Lebanon War.

Hybrid warfare needs NATO "to be prepared for the unexpected" according to Professor Julian Lindley-French's words, and it requires a different and adapted approach in the strategic and operational NATO's strategy. Considering the above, my work pursues a specific analysis of

NATO's strategies and operational tools to prevent and fight hybrid threats from both State and non-State actors.

A consequent objective of this analysis will be the evaluation of the efficiency and effectiveness of NATO's response to the new hybrid security environments and actors. The policy and military evaluation will lead to synthetic and punctual recommendations on the topic for the Organization, experts and policy-makers to implement and improve NATO's capabilities.

The paper intends to answer to the following investigation questions:

How NATO face hybrid warfare threats from state and non-state actors?

Which are NATO's conceptual approach and instruments against hybrid warfare? Is there a difference in its response, related to the different type of actor? How effective is NATO's response to the new security environment?

To answer, the methodology applied is a qualitative approach, based on an accurate selection of policy papers, articles, NATO's official publications and academic essays. Moreover, the paper addresses a specialized audience, as NATO's experts and academics and policy-makers, to whom are especially oriented the final recommendations.

2. The current hybrid security environment

In 1992 Francis Fukuyama [1]said that history had ended: so much happened in the 20th Century to leave no space to imagination. And yet, the new century is as full of events as we couldn't expect. The implosion of Union of Soviet Socialist Republic (URSS) marked the beginning of a period in which the United States of America (US) became the hegemon of the international system, configuring an unchallenged supremacy. However, history was not done, and in 2001 with the 11/9 Twin Towers attack in New York, the West realized a new era started.

The current international system is much more complex and volatile, new actors and threats, in a faster, interconnected and interdependent world. The new multipolar order, resulting from

[1] Fukuyama, F. *The End of History and The Last Man*. New York and London: The Free Press, 1992. Looking today at Fukuyama's perspective on a unipolar world order, where liberal capitalistic democracies establish a durable and unchallenged system, highlights instead the deeply unstable and changing nature of the world system, in particular, the deep crisis that invested Western liberal democracies, values and identity and the spread of populism and nationalist movements, the increasing importance of private and transnational actors.

the slow decline of the US as hegemon and the rising of Eastern powers, especially China, reflect itself on a new security environment, deeply influenced by advanced technological development and globalization. State borders are no longer a barrier as cyber space cannot be delimited and transnational crime networks are tangled and worldwide spread. Security threats today do not mostly come on tanks and war declarations and the once clear definition between war and peace is more and more vague, fact that makes a response, as much political as military, complicated.

The Western security culture in the past Century has been used to traditional military threats, based on clear distinctions: enemy-ally, war-peace, foreign-domestic. As analysed by Hoffmann in Hybrid Warfare and Challenges[2], the US, as the most powerful Western military force, has over invested in state-based security threats and traditional war methods, as defined by Hoffmann as "myopic preoccupation with conventional war", while instead, it needs to pay more attention to new challenges.

The current security scenario has dramatically changed, and it keeps evolving rapidly, where the agenda is broader, as progressively the concept of security includes new issues, and deeper, as new actors, supra-state and sub-state emerge influencing the global agenda. Individuals are increasingly acting as security actors: terrorist groups and foreign fighters, transnational crime. In the Post-Cold War, state power and sovereignty are being eroded[3], still pillars of the international system, yet debilitated by the progress made by international law, human rights protection and international intervention. The so-called R2P, Responsibility to Protect, still controversial in the broader mark of United Nations (UN), has attacked the former absolute concept of sovereignty, and contribute to the approach of human security, a new multi-dimensional, multi-level approach to security, where the individual replaces the state at the centre of the system.

9/11 have had a huge impact on the evaluation of non-state actors as seriously able to pose a threat to legitimate states. Non-state actors and failed states, state-backed groups, self-founded groups, using new technology and advanced techniques, can effectively engage a full range war, as nation-states are developing irregular warfare methods, therefore the categorization of state as traditional forces and non-state ones as irregular, is nowadays obsolete.

[2] Hoffman, F. *Hybrid Warfare and Challenges*. New York. Joint Forces Quarterly 52, First Quarter 2009.
[3] Hirst, Q. P. *Another Century of Conflict? War and the International System in the 21st Century.* Birbeck College, London. 2002.

Every Era has its type of war, its instruments and strategies. The 2001 Twin Tower Attack, the 2006 Lebanon War and the 2014 Ukraine war, have shown a new, intensified, kind of warfare. If the Industrial Revolution changed the way of conflict during the last century, today the Revolution in Military Affairs (RAM[4]), is about advanced technology, but not only. In fact, the big difference found in the nowadays challenges is the complex fusion of so different techniques, actors, instruments. What is been called, *Hybrid warfare*. As Frank Hoffman says, "Hybrid wars are not new, but they are different". No more one single approach to war, instead, the proliferation of several and different methods, instruments, acting synchronized, strategically integrated. Western strategists have always had a military-oriented, conventional, technical approach to war, consequently, hybrid is a word created by a western perspective, responding to a non-Western way to engage war, an "irregular" approach.

The rise of hybrid threats and warfare needs to be contextualized in the more general changing scenario of warfare forms in recent years. As called by William Lind[5], in the last decades war has evolved in the Fourth Generation, consisting in three core political elements: "The state loses its monopoly on war; Fourth Generation warfare is marked by a return to a world of cultures, not merely states, in conflict; At its core lies a universal crisis of legitimacy of the state, and that crisis means many countries will evolve Fourth Generation warfare on their soil".

2.1 Hybrid warfare, a Western perspective

The word *hybrid* warfare became very much (mis)used in the academic and press context just after the Crimea War in 2014, while before it was part of military and strategic academic studies. was being used in academic context already at the beginning of 2000, but just after 2014 Crimea war it became very much used by the Western press.

Frank G. Hoffmann represents one of the major experts on War studies and hybrid warfare and threats, serving at the National Defence University as a Distinguished Research Fellow with the Institute for National Strategic Studies, Washington DC.

Hoffmann's conceptualization of hybrid warfare is the most accepted in the academic and community: "a full range of modes of warfare, including conventional capabilities, irregular

[4] Hirst, Q. P. Op. Cit.
[5] S. Lind. William. *Understanding Fourth Generation War*. Military Review. September – October 2004. http://www.au.af.mil/au/awc/awcgate/milreview/lind.pdf

tactics and formations, terrorist acts that include indiscriminate violence and coercion, and criminal disorder. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical *and* psychological dimensions of conflict (…)".

Hybrid threats and warfare analysis are born by looking at the enemy[6], Western defence planners and experts created the term describing non-Western war behaviour in the recent armed conflict, in Iraq, Afghanistan, Lebanon, Chechnya, Ukraine. In particular, the American perspective on the rise of hybrid warfare interprets the superiority of the American military force as an incentive for non-state actors to develop alternative military and non-military tactics to overcome their inferiority. As described in the Joint Operating Environment[7] "The continued dominance of America' s armed forces in large-scale force-on-force warfare provides powerful incentives for adversaries to employ methods designed to offset our strengths. From non-state actors using highly advanced military technology and sophisticated information operations, to states employing unconventional technologies, to the improvised explosive devices that pose grave threats to our troops, smart adversaries will tailor their strategies and employ their capabilities in sophisticated ways." And more about Western vision in the words of US Army Colonel Brown[8]: "One could argue that hybrid warfare emerged because of the United States 'dominance in traditional warfare with a superior technological advantage in sensors, shooters, and battle command. The enemy is not stupid and gets a vote on how it will fight against the US and its allies."

Agreed to the hybrid nature of future conflicts is Russel Glenn[9] in the analysis of Second Lebanon war in *All Glory Is Fleeting: Insights from the Second Lebanon War,* where he stated the superiority of Hezbollah against the Israelite military has been given by the mix of simple and sophisticated tactics, the agility of planning and execution, against which the conventional state forces have been "futile". Categorization of war modes, tactics and instruments are useless in the modern war analysis because all factors tend to converge and blend together. Hybrid, blurred type of war which requires defence planners to go beyond conventional state-based war, being prepared and engaging not only military instruments but total wars, which aim to be disruptive not only on the battlefield. Hybrid warfare involve a full range of elements,

[6] Hoffmann. Op. Cit.
[7] Department of Defence. *Joint Operating Environment*. Joint Forces Command, February 2010. p.66
[8] Leslie, F., Brown. *Twenty-Frist Century Warfare will be Hybrid*. US Army College, March 2011, 14
[9] W. Glenn, R. *All Glory Is Fleeting: Insights from the Second Lebanon War.* Santa Monica. 2008. p.73.

orchestrated to act in a coordinated, coherent and simultaneous way, creating a powerful synergic effect, boosted by use of modern technology.

Among the challenges posed by hybrid warfare at the operational level, there is the ability to keep the battlefield as far as possible from civilian population, fact that has been increasingly exploited by terroristic and non-conventional forces during the last decades. Furthermore, the use of technology as an informational and learning instrument for this kind of irregular combats, who study and acquire new techniques and weapons thanks to the Internet sources.

Hybrid threats are largely use by non-State armed groups (NSAGs), State or non-State backed, represent new influent actors in the security context, revealing themselves powerful and dangerous enemies especially in the Middle East and North Africa recent conflicts. Often competing with state forces, these groups have developed asymmetrical tactics, based on multi-layered activities. As the final objective is not only a win on the battlefield, but often the creation of an alternative model of governance, the NSAGs attack the state in a full spectrum war: legal conventional- military capacities, political propaganda, but also illegal instruments as terrorism, guerrilla, subversion, organized crime and cyber warfare, these are just some of the most used elements.

However, it is not only non-state actors groups engaging hybrid warfare, but also states increasingly use hybrid methods to pose indirect threat for strategic aims with the advantage of avoiding direct danger of getting into war. In fact, without a recognizable aggression or a indentifiable aggressor, as it happens with cyber-attacks, war would be impossible.

Although traditional and conventional conflict will probably still be the largest part of future conflicts, the hybrid approach represents a complicating factor in the defence planning. It requires a multi-perspective approach to conflict, more dynamic, flexible and adaptable.

2.2 Hybrid, old war, new word?

As Clausewitz said in his masterpiece “War is more than a true chameleon that slightly adapts its characteristics to the given case”[10]. Beyond the contexts of war, that change over the centuries, war maintains its nature, which the military philosopher recognized as three principal

[10] Von Clausewitz, C. *On War*. Princeston. 1832

elements: violence, chance and probability and political considerations. If war is always war, no matter the circumstances and the modes in which it happens, what does it mean *hybrid*?

As on one side the term has become more and more (ab)used in the Western military, academic literature and the media in the past decade, on the other side many believe that it is just a catchword lacking conceptual clarity. As a concept, hybrid warfare seems to refer to a wide range of war tactics, instruments and strategies that do not contain anything especially new. According to Damien Van Puyvelde, the over-use of the hybrid word generates confusion and ambiguity, instead of clarifying the nature of modern warfare. And as he adds "Any threat can be hybrid as long as it is not limited to a single form and dimension of warfare." [11]In his analysis, Puyvelde highlights the importance for Western strategists to focus on the complexity of modern threats, avoiding simplifying specificity in one sum-up word.

In accord with Puyvelde on the emptiness of the hybrid concept, Colin Gray argues that future wars will basically be the same, considering that since men fought wars, the mix of conventional and unconventional means have been always used with the aim of exploiting enemies' weaknesses, therefore the concept of hybrid warfare is nothing new[12]. Surely, innovation in technology, bring up new challenges and ways, as cyber warfare, however, the objectives of war itself does not change, besides innovative ways to achieve them.

Nonetheless, the concept of hybrid warfare is born in Western military strategist and experts because of the need to define a non-traditional approach to warfare, coming from non- Western powers, which revealed themselves dangerous threats in the last decades, especially in the 2008 Second Lebanon War and in 2014 Crimea war. The Western approach to warfare has always been focused on military force and violence[13], consequently the latest evolution of warfare and threats towards a convergence of means and instruments, which include aspects of society other than the military, as economic and political, found the West quite unprepared. As a result, experts started looking for a definition of this changing threats, as the clarification of the concept could lead to a better ability to conceive an efficient counter-strategy. In this perspective, the concept of hybrid warfare, beyond the discussion of how new or old it is, can be useful in the defence analysis and planning.

---

[11] Van Puyvelde, D. *Hybrid warfare- Does it even exist?* 2015. NATO Review magazine online. https://www.nato.int/docu/review/2015/also-in-2015/hybrid-modern-future-warfare-russia-ukraine/en/index.htm

[12] Gray, C. *Another Bloody Century: Future warfare*. London, Weidenfeld and Nicolson, 2005

[13] Kitzen, M. *Western Military Culture and Counterstrategy: an Ambiguous Reality*. Netherlands Defence Academy, Department Military Operational Art and Science. 2012.

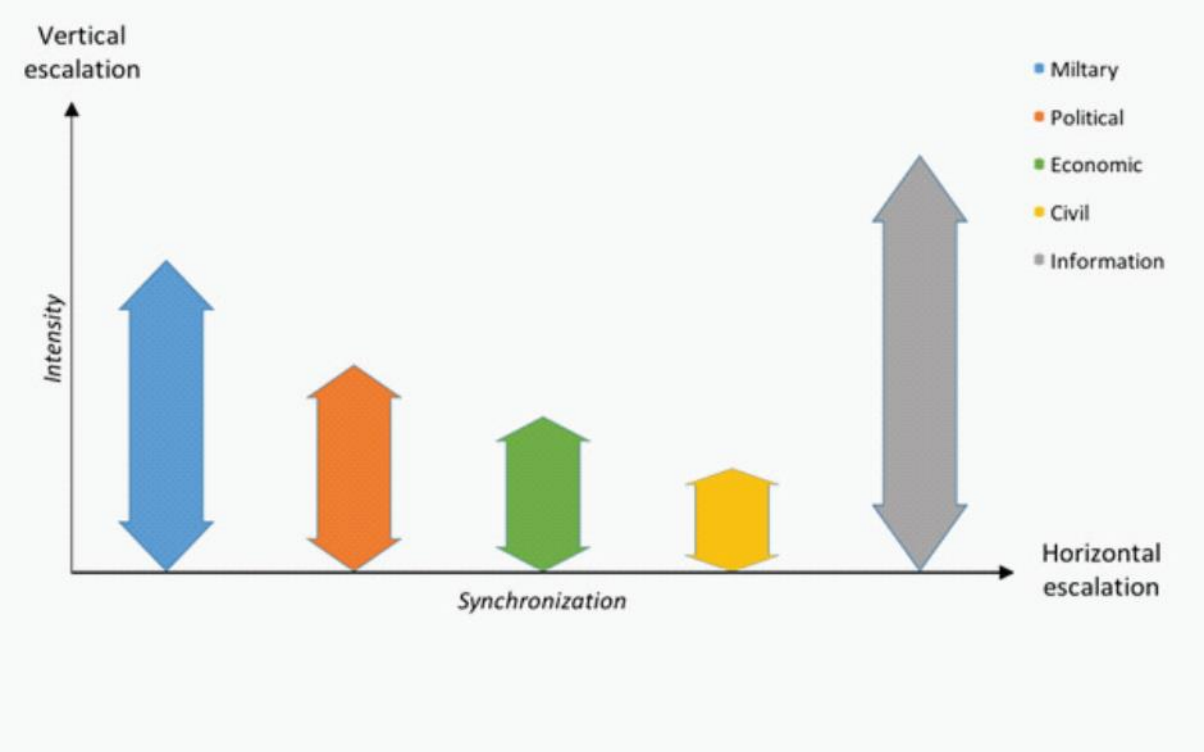

Image 1. **Hybrid Warfare Model**

Source: NUPI Policy Brief[14]

Among the core characteristics of hybrid warfare, the development of non-military instruments representing a horizontal escalation[15] of coordinated unconventional elements, the model[16] represented in the image above describe analytically hybrid warfare as "*asymmetric and multi-modal along a horizontal and a vertical axis, and to varying degrees shares an increased emphasis on creativity, ambiguity, and the cognitive elements of war*. Synchronization and intensity of military and non-military elements, as political, economic, civil and informational, are combined by hybrid actors to create a powerful synergetic effect, able to attack the enemy on different levels at the same time.

Therefore, beyond the debate about the derivation of the concept of hybrid warfare, an analytical examination of recent, conflicts can lead to a clearer understanding of the set of

[14] Reichborn-Kjennerud, E. Cullen, P. NUPI- Norwegian Institute of International Affairs. Policy Brief*, What is Hybrid warfare. 2016.*
[15] Reichborn-Kjennerud, E. Cullen, P. Ibid.
[16] Reichborn-Kjennerud, Cullen. Ibid.

modern challenges, distinguishing its components and the way they act together, and consequently enhance the defence thinking and planning. As the term hybrid came from the description of the enemy' tactics[17], experts should take it as an advantage to improve defence weaknesses and learn from enemy's strengths.

2.3 NATO, a 20th century organization in the hybrid Era

NATO, the North Atlantic Treaty Organization, being the strongest Western Defence Organisation is the primer addressee of the new security environment and its challenges. The profound changes that have occurred in the International Relations field after URSS collapse and the end of the Cold War, led to a slow but constant decline of the West as a political and civil power, affected by a deep crisis, its values and identity. A political and identity crisis for liberal democracies which blend within a complex and highly instable international context. The weakness of sovereign states, their increasing internal fragmentation and external mistrust feed the precariousness of the current international system. However, globalization with constant and unlimited exchange and interdependence in contemporary societies crushes with the increasing nationalist protectionism tendency. Potential adversaries take advantage of the globalised context, establishing new and unexpected collaborations, helped by communication and technology, media manipulation as form of self-legitimization and discredit for NATO as analysed in NATO ACT Report *MCCHT*[18]. In this contradicting and complex scenario, it is certain that states cannot overcome modern challenges by themselves. The cooperation that Western powers have engaged since WWII in the security and defence field is still, and perhaps more than ever, essential and necessary for confronting new threats. That is why NATO, its updating to the current challenges, which are so different from the ones that NATO was born for, and strengthen its capacity to learn and adapt, is essential.

Despite NATO's military superiority based on massive military expenditure[19], estimated at 936 billion dollars in 2018, with a rise of 53 billion since 2014, new threats pose a real danger for the Allied. The first discussion on the concern of the Alliance regarding hybrid threats and warfare emerged at the 2010 Lisbon Summit and in the adoption of the 2010 Strategic Concept,

[17] Hoffmann, F. Op. Cit.
[18] NATO ACT Report - *Military Contribution to Countering Hybrid Threats (MCCHT), 3-4.* August 2010.
[19] NATO- Press Release, Public Diplomacy Division. *Defence Expenditure of NATO Countries (2011-2018)*. 10 July 2018. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180709_180710-pr2018-91-en.pdf

addressing emerging security threats and its hybrid nature[20]. NATO members are divided, despite an almost general forms of government homogeneity, by different specific security and defence issues dealing with geopolitical and geographic reasons, but also resources and power, do share values and objectives.

Since its creation in 1949, the Alliance has guaranteed in the North American and European zone a strong, durable and safe peaceful community, establishing its strength in the international scenario on military superiority.

As analysed above, the set of new challenges has deeply changed in the last decades and NATO recognizes the necessity to evolve itself, strategically and operationally, to be adaptable and agile[21]. What is sure is that no single state today, no matter how strong it is, can face alone kind of threats that are multi-dimensional, transnational, complex and interrelated.

Ethnic, cultural and social aspects are increasingly important in conflict scenario; therefore, NATO strategies and operations are required to improve their ability to work with civilians, collaboration with local/regional and international organization, first the United Nations and the European Union to achieve a comprehensive approach[22] to crisis situations and threats. As stated in the 2010 Strategic Concept, p. 14, point 17, "Deterrence, based on an appropriate mix of nuclear and conventional capabilities, remains a core element of our overall strategy". Traditional military forces remain the major Alliance's strength, however, the key for success in confronting hybrid foes is the develop of a new mindset, through investigation and study of adversaries' strategies and capabilities.

Researchers and strategists [23]argue that hybrid threats and warfare go beyond physical battlefield towards a "cognitive realm", i.e. cyber-attacks, high-tech wars that lead to "unrestricted warfare[24]" in which "there are no rules, with nothing forbidden".[25] In an unlimited war scenario, where military blend with politics, economics, religion and diplomacy, conventional weapon and old deterrence and defence strategy, are not enough. Western conventional approach is out-of-date.

[20] NATO- Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. 2010. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf
[21] NATO ACT (MCCHT). Op. cit.
[22] NATO ACT (MCCHT). Op. cit.
[23] Liang, Qiao. Xiangsui, Wang. *Unrestricted Warfare*. Beijing. PLA Literature and Arts Publishing House. February 1999.
[24] Liang, Q., Xiangsui, W. Ibid.
[25] Liang Q., Xiangsui, W. Ibid. p.2.

In the words of Williamson Murray and Allan Millet[26], the formula for success is a military culture that embrace innovation. NATO ability to stimulate a culture of innovation and research is fostered by its members' diversity, a favourable key element to mix different military cultures and strengths into one powerful multi-faceted strategy.

3. NATO: reinvent to survive

3.1 NATO conceptual and policy strategy

To understand and define the conceptual and policy strategy that NATO adopts, it is necessary to deepen the vision of NATO as a multi-governmental organization. A common strategy is the result of a complex negotiation of interests, visions, resources and power, fact that inevitably affect the results.

NATO Strategic Concept [27]is a strategic and conceptual guide-map for the Organization. In the 2010 Document, the Allies agree about the changing nature of the current context and features of the future security environment, addressing "new emerging challenges", as international terrorism, transnational organized crime, cyber and technological threats and environmental emergency.

However, threats they pose to the Alliance and to the single Members, are described as not as dangerous as the one previously faced, i.e. Soviet Union. The new kinds of security threats, beyond the military, appear to be underestimated. Instead, the academic analysis, under the name of deepening and widening process [28], already integrates non-military issues in the global security scenario.

"Today, the Euro-Atlantic area is at peace and the threat of a conventional attack against NATO territory is low. (…) However, the conventional threat cannot be ignored". [29]From this extract, it is clear that a real threat is still identified as conventional- military. In the following points

[26] Murray, W. Millett, A. *Innovation: Past and Future in Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.
[27] NATO Strategic Concept – Op. cit.
[28] Buzan, Barry. Hansen, Lene. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press, 2009.
[29] NATO Strategic Concept – Op. cit.

of the Concept, nuclear proliferation and other weapons of mass destruction are addressed as the most dangerous threats to NATO zone and global security.

NATO recognizes the existence of new actors and non-military phenomenon that challenges the Alliance, however, when it comes to security threat, it is related just to conventional- kinetic external issues, as nuclear weapons proliferation in non-NATO zone. Also, in the legal framework, Article 5 and collective security concept is linked just to external military threats on NATO territories.

However, hybrid threats, as dealt above, may not come on tanks and missiles, but in a much more complex and blurred form, growing inside national borders, inside Western societies. It is consequently difficult to establish in which cases Article 5 would be applicable, apart from external military aggression, in case for example of cyber-attack[30]. NATO ability to respond effectively and rapidly is a doubt among experts[31]. A primary problem is that NATO today finds itself, as inter-governmental and military organization, projected in a multi-dimensional and interrelated network of actors and threats that go beyond military, therefore fall outside its mandate, but still need to be managed by NATO to succeed in its main objectives.

Therefore, NATO needs a new perspective in its strategy, to understand the new challenges at first and then innovate its own instruments and capabilities towards a comprehensive approach[32]. As Miklaucic brilliantly points out, "many of the perceived threats (terrorism, trans-national crime, violent extremism) are symptoms or consequences of underlying root causes (poverty, ethnic strife etc). (…) Whereas treating the symptoms is about preventing actions in the shorter term, addressing the root causes of instability is about changing conditions in the longer term, which is the fundamental goal of development."[33]

Although treating deep causes of threats is not competence of a military organization, and it would require a far more difficult dialogue and consensus in a multi-lateral forum, it is increasingly important for NATO to collaborate with non-military organizations and civilians to better understand deeper causes while operating on the symptoms[34].

[30] Aaronson, M., Diessen, S., De Kemabon, Y., Long M., B., Miklaucic, M. *NATO Countering the Hybrid Threat*. Washington DC. PRISM- Center for Complex Operations at National Defence University. VOL.2. Sept. 2011.
[31] Aaronson, M., PRISM- Op. Cit.
[32] Miklaucic, Michael. *NATO Countering the Hybrid Threat*. NATO Allied Command Transformation. Sept. 2011
[33] Mikaucic, M., Ibid.
[34] Mikaucic, M., Ibid.

Collective defence and crisis management [35]are fundamental cores on which NATO bases its deterrence and defence strategy, however, confronting hybrid threats require the development of new capabilities and an extensive approach.

The Comprehensive Approach [36]as conceptual strategy on hybrid threats is still relatively undeveloped and generic about "comprehensive activities[37]", non-military, involving civil society and private sector. The political dimension of the comprehensive strategy is decisive while military becomes a support tool; in fact, political and diplomatic instruments need to be strengthened by keeping NATO military lead, as hybrid threats operates on different levels, among government, society and military force[38]. "NATO must adapt its capabilities to its adversaries and not expect adversaries to adapt to NATO"[39], that means the creation of a solid strategy of countermeasure against hybrid threats, keeping in mind that political and military effectiveness are crucial, as "political decision-making must not take longer than it takes to move forces"[40]. However, finding agreement and fast resolution at the NATO top political summit is hard to achieve, unless a situation of extreme gravity occurs, fact that obstructs the achievement of a concrete comprehensive approach.

Hybrid threats and warfare push NATO and its Members to evolve on many aspects, not only dealing with NATO approach to exterior foes, but also its internal coherence and solidity. Minimizing Alliance's vulnerabilities needs to be an important part of the comprehensive strategy, fighting internal corruption, reinforcing a common shared point of view among the Members, all based on a solid combination of "diplomatic, informational, economic and military tools (DIME[41])".

Important aspects for the new NATO security strategy approach have been defined during the Wales Summit in 2014, when The Readiness Action Plan (RAP) was presented. "In order to ensure that our Alliance is ready to respond swiftly and firmly to the new security challenges, today we have approved the NATO Readiness Action Plan. It provides a coherent and comprehensive package of necessary measures to respond to the changes in the security

[35] NATO Strategic Concept – Op. cit.
[36] Mikaucic, M., Ibid.
[37] Mikaucic, M., Ibid.
[38] Lindley-French, Julian. *NATO and New Ways of Warfare: Defeating hybrid threats*. NATO NDC Conference Report. Research Division – NATO Defence College. May 2015
[39] Lindley-French, J. Ibid.
[40] Lindley-French, J. Ibid.
[41] Lindley-French, J. Op. cit.

environment on NATO's borders and further afield that are of concern to Allies" states the Wales Summit Declaration[42].

During the Summit, the Alliance recognized new security threats to the Euro-Atlantic space coming from two flanks, Eastern ones concerning Russia and South ones, concerning North Africa and the Middle East. The RAP contains two new measures especially made to counter this kind of threats: Assurance and Adaptation Measures[43], both dealing with changes in military presence, increased numbers of NATO forces in Central and Eastern Europe and Turkey, but also structural changes to military capabilities. Particularly, Adaptation Measures include the implementation of NATO Response Force (NRF)[44], with an increased number of land, air, sea and special forces and their capability to be deployed in a quick-reaction to attack, as guaranteed by the Very High Readiness Joint Task Force (VJTF). [45] Moreover, NATO expands its network of multinational headquarters in Eastern Europe Allied territories, already settled in Hungary and Slovakia since 2015, NATO Force Integration Units" (NFIUs) are now based also in Bulgaria, Estonia, Hungary, Latvia, Lithuania, Poland, Romania and Slovakia.

The measures mentioned above adopted by NATO in 2014, demonstrate NATO's consciousness about the evolving security environment and the necessity to enhance its ability to react and response quickly, being adaptable and flexible to a full range of threats that leave no time to hesitation.

3.2 NATO operational and military tools

Above it is analysed the creations, main elements and issues of NATO's strategy about hybrid threats. In this section, it will be described how this strategy is concretized in military tools and operational programs.

First, as military organization, NATO concretizes its capabilities in terms of military forces. After the Twin Tower Attack in New York in 2001, at Prague Summit in 2002 NATO Heads of State and Government decide to step up NATO capabilities and create NATO Response Force (NRF) "consisting of a technologically advanced, flexible, deployable, interoperable and

[42] NATO- *NATO's Readiness Action Plan*. Fact Sheet. NATO website. July 2016.
[43] NATO- *NATO's Readiness Action Plan*. Op. Cit.
[44] NATO – *NATO Response Force.* NATO Website,16 July 2017. Retrieved from *https://www.nato.int/cps/ua/natohq/topics_49755.htm*
[45] NATO – Supreme Headquarters Allied Powers Europe. *NATO Response Force / Very High Readiness Joint Task Force.* April 2018. Retrieved from https://shape.nato.int/nato-response-force--very-high-readiness-joint-task-force

sustainable force including land, sea, and air elements ready to move quickly to wherever needed"[46]. NRF is created with the objectives of fast responsiveness to crisis emergency to collective defence, therefore covering a great spectrum of challenges and scenarios. To respond to different contexts and necessities, the NRF is composed by different operational sections, each corresponding to a specific aspect. First, the Rapid Deployable Corps[47] set in nine High Readiness Headquarters, controlling sixty thousand soldiers considered to be ready within ten days to a complete deployment of two months.

Also, part of the NRF, is the NATO Special Operations Forces (SOF), [48]directed and coordinated by NATO Special Operations Headquarters (NSHQ) with its operational centre in Mons, Belgium at Supreme Headquarters Allied Powers Europe (SHAPE). As a powerful military operation command, NSHQ include full range of operational aspects "NSHQ is a unique hybrid organisation. It is involved in a very diverse set of activities such as SOF-specific intelligence, aviation, medical support and communications."

The NRF was born as an answer for the 21th Century changing security environment, where already in the first years of the new century NATO realized the necessity for a structural change in its capacity and means. Fallen the Soviet Union as a conventional military threat especially for Easter Europe, during the Prague Summit the Members identified a set of emerging unconventional *hybrid* threats, such as transnational organized-crime and international terrorism, which imply for NATO the necessity to start a process of renovation through self-reflection, "this is not business as usual, but the emergence of a new and modernised NATO, fit for the challenges of the new century" as stated by former NATO Secretary General, Lord Robertson.[49]

The new command structure under the NRF program decentralized its previous base in Virginia, United States, to split it and open new command centres in four different areas among the US and Europe, all under direct operational and strategic responsibility of the Allied Command of Operations (ACO). As the new threats are borderless and spread, NATO new command is built with a "global mind-set"[50]aims for high responsiveness everywhere. Moreover, the NRF is totally new in its nature, representing a combined coordinated multi-

[46] NATO – Prague Summit Declaration. November 2001. NATO website. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_19552.htm
[47] NATO – retrieved from https://www.nato.int/cps/ua/natohq/topics_50088.htm
[48] NATO – retrieved from https://www.nato.int/cps/ua/natohq/topics_105950.htm February 2015.
[49] NATO Review- Jones, L., J. Ibid.
[50] NATO Review- Jones, L., J. Ibid.

nature of land, maritime, air forces, deployable for any kind of mission, while the old-style NATO forces were usually built for specific regions and missions.

As how innovative and efficient as it appeared, the NRF analysed in 2018, fourteen years later, did not mean the expected in the NATO operational innovation process. Used just in "non-combat operations of limited importance"[51], the NRF initial enthusiasm quickly fell in general criticism and disappointment[52]. In fact, lack of political willingness [53]and effort caused by a deep problem at NATO's roots, i.e. the different consideration and importance attributed by its Members to the Alliance and the consequently different endeavour that each state put in NATO's projects, in short: lack of unified aim and perspective. "In many ways, the NRF represents a microcosm of the broader discussions characterising the Alliance"[54].

Especially after the speech of Russian President Putin during the Munich Security Conference in February 2007[55], NATO Members concerns started diverging about where NATO capabilities would be need the most: while many European countries felt threatened by Putin's declarations and therefore were calling for "NATO at home", others, approved the more globalized security agenda of NATO' renovating process, dividing NATO in two factions, "the globalizers" and the "Article 5ers"[56].

The divergent perspectives on which objectives, resources[57] and use the NRF should have had, contributed to weaken the project. Despite being born to innovate NATO operational capabilities, the NRF reflected the old Western warfare style, based on military high technological superiority, used to interstate armed conflicts; therefore, this focus was at the base of the NRF's conception in 2002. However, when it came to practice, the NRF was

[51] Lasconjarias, G. *The NRF from Key Driver of Transformation to a Laboratory of the Connected Forces Initiative.* NATO Research Paper – Research Division, Defence College. Rome. January 2013.
[52] Ringsmose, J. *Taking Stock of NATO's Response Force*. NATO Research Paper- Research Division, Defence College. Rome. January 2010.
[53] Ringsmose, J. Op. cit.
[54] Ringsmose, J. Op. cit.
[55] Shanker, T. Landler, M. *Putin Says U.S. Is Undermining Global Stability.* The New York Times. February 2007. Retrieved from https://www.nytimes.com/2007/02/11/world/europe/11munich.html
Accused by the US to contribute to the Middle East unstable situation and endanger global security, President Putin replied: "The process of NATO expansion has nothing to do with modernization of the alliance," and "We have the right to ask, 'Against whom is this expansion directed?".
[56] Ringsmose, J. Ibid. p. 6
[57] Macias, A., W. Schoen, J. *Trump pushes NATO allies to increase spending as US share of funding slows.* CNBC. July 2018. Retrieved from https://www.cnbc.com/2018/07/10/trump-pushes-nato-allies-to-increase-spending-as-us-funding-slows.html
More about resources and financing disagreements, see the latest NATO Summit where US President Trump urge European NATO members to increase their NATO contributions.

deployed for stabilization and reconstruction missions far from home[58], making evident that the concept, resources and equipment were not adequate to the aim it was created for, the NRF needed a review. Between 2008-2009 the NRF was reformed and what it results was a smaller restructured [59]form of the NRF, which kept its name, with a total personnel number cut to the half of the initial assessment.

As analysed by Lasconjarias, the core word around which the NRF turns is interoperability[60], meant as a continue process of integration, development and coordination among units, services and forces, a high-cost effort to combine not only materials and tools, but also approaches, North American and European, to enrich the technical, but also conceptual, NRF's capacity to be a truly useful instrument. "The work shared between Americans and Europeans at all levels- strategic, operational, tactical and technical – make the NRF a true laboratory for forging interoperability. [61]"

Despite its initial stalemate, the 2009 renewal and reorganization of the NRF seems to have brought positive effects: partnerships with non-NATO countries, like Finland[62] are increasing and the exchange of knowledge and methods benefits the Alliance's forces. In fact, despite the NRF's issues[63], mostly dealing with military issues, like shortages of forces, and political disagreements, it represents also "unique forum of exchange[64]".

Fostering cooperation among European and US forces, exchange of knowledge, techniques and technology, to fight new common threats also enhance the now fragile political and diplomatic relations within the West, affected by the US's pivot to the Orient[65].

The creation of the NRF was both an answer and an effect of a security scenario changing, the erosion of the Western Allied block and the threatening appearance of new powerful actors, weapons, warfare methods. NATO's recognition of the new situation in the early 2000s led, on the operational and technical side, to an overambitious NRF project. The NRF became a metaphor of NATO's usefulness in 20th Century and its capacity to survive. Both new external

[58] Lasconjarias, G. Ibid. p. 4
[59] Lasconjarias, G. Ibid. p. 5
[60] Lasconjarias, G. Ibid. p. 6
[61] Lasconjarias, G. Ibid. p. 6
[62] The Finnish Defence Forces Website. *NATO's Partnership for Peace.* Retrieved from https://puolustusvoimat.fi/en/international-activities/natos-partnership-for-peace-programme
[63] Ringsmose, J. Ibid. p. 4
[64] Lasconjarias, G. Op. Cit. p. 7
[65] Lasconjarias, G. Ibid. p. 7

threats and the pressure of different interests and perspectives coming from inside the Alliance, pushed the NRF program expectations, as if its success would represent a broader NATO's reaffirmation of itself. "(…) The debates and disagreements about the NRF are closely mirroring the wider discussions about the future of the Atlantic Alliance: overall political inclinations are clearly reflected in the positions takes by the allies in the deliberations about the response force. (…) This means that the NRF is just as affected by strategic schizophrenia as the Alliance in general."[66]

4. Cases studies: engaging hybrid warfare

Following a selection of two cases of study, which are emblematic examples of how a State-actor such Russia, and a non-State actors as Hezbollah and more in general, terrorist groups, engage and develop hybrid tactics in modern conflict. As cases of study, Russia, considered one of the few states which employ effectively hybrid warfare, especially cyber warfare. In the Middle East, private groups successfully strengthen their military capabilities, bypassing international law, gaining international status. The study of these two actors is fundamental to understand potential adversaries' mind-set, and therefore important in the creation of an effective counterstrategy for NATO.

4.1 Russia, state actor engaging hybrid warfare

Talking about hybrid warfare during the last decade, it means talking about Russia. Centre of debate, analysis and concern among Western foreign policy and defence experts, but not only, Russian activities in Eastern Europe grew progressively for intensity and quantity, in what it seemed to many a clear attempt to recreate its Soviet sphere of influence, by using conventional and non-conventional means[67]. Russian foreign policy in the last two decades has shown a crescendo of aggressiveness against the Eastern Europe neighbours[68], starting from "energy

[66] Ringsmose, J. Ibid. p. 8
[67] Cooley, A. *Whose Rules, Whose Sphere? Russian Governance and Influence in Post-Soviet States*. Carnegie Endowment for International Peace. June 2017. Retrieved from https://carnegieendowment.org/2017/06/30/whose-rules-whose-sphere-russian-governance-and-influence-in-post-soviet-states-pub-71403
[68] Traynor, I. *Russia accused of unleashing cyberwar to disable Estonia.* May 2007. Retrieved from https://www.theguardian.com/world/2007/may/17/topstories3.russia. A crucial antecedent of Russia threatening

cut-off, economic warfare, financial and social destabilization, cyber offensives and more"[69] up to Crimea war and annexation in 2014, which has been addressed as "the most dangerous situation in East-West relations since the Soviet invasion of Czechoslovakia in 1968"[70]. Military reaction from NATO was expected, but Western political leaders saw Ukraine as the political issue and the necessity to avoid "the abyss of military escalation" as declared by German Foreign Minister Frank-Walter Steinmeier, therefore leading to a diplomatic reaction in form of economic sanctions.

Beyond geopolitical and strategic reasons, the Crimea War made the hybrid warfare term famous. In fact, before 2014, the term hybrid warfare was used for non-state actors asymmetrical fighting tools and techniques, but Russia proved that a state-actor can use powerfully a combination of military and non-military means, exploiting the capacity of a nation-state to mix soft and hard power, intimidating and deterring without using military force, but still being ready to deploy it[71].

Despite Russia progressive strengthen of its military capacity, realized by an almost total transformation[72] of its armed forces since 2008, its main strength lies in the ability to read the moment and combine necessity and opportunity[73]. Russia did not only boost its armed capacity, but also invested in advanced technology, particularly: "web-based information technologies, instant mass communications, computer hacking, cyber warfare to damage foreign information infrastructure"[74]. A perfect strategical analysis of maximizing profits and minimizing risks and costs, that got unprepared the West and NATO, and opened a concerned debate on the hybrid warfare as real threat coming from the old enemy in a new potentiate version[75].

Russian hybrid warfare is not limited to a battlefield, instead it is used as an instrument of foreign and security policy [76] rooted in Russian-identity created in opposition to the West,

---

hybrid capability is represented by massive cyber-attacks in 2007 against Estonia, an alarming event for the West.

[69] Giles, K. *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power.* Research Paper, Russia and Eurasia Programme. March 2016.

[70] Apps, P. Ukraine crisis gives NATO, West no good options. Reuters online. March 2014. Retrieved from https://www.reuters.com/article/us-ukraine-crisis-west-analysis-idUSBREA210G420140302

[71] Lasconjarias, G., A. Larsen, J.(eds). A. Ruitz Palmer, D. (author). *Back to the Future? Russia's Hybrid Warfare , Revolutions in Military Affairs, and Cold War Comparisons* as part of Research Paper, *NATO's Response to Hybrid Threats*, NATO Defence College. December 2015. p. 50

[72] Giles, K. Op. Cit. p. 3

[73] Lasconjarias, G., A. Larsen, J. Ibid. p. 50

[74] Lasconjarias, G., A. Larsen, J. Ibid. p. 51

[75] Lasconjarias, G., A. Larsen, J. Ibid. p. 51

[76] Lasconjarias, G., A. Larsen, J. Ibid. p. 52

perceived as ideologically opposite and strategically hostile, creating a relation of zero-sum security conduct[77].

Despite many discord opinions about how new are the warfare elements used by Russia in the Ukraine War, for example The Swedish Defence Research Agency (FOI)concluded in its studies of the Crimean operation: "calling it new reflects a failure of imagination, rather than novel Russian military capabilities"[78], the West and NATO in particular recognize in the Russian aggressive and self-assertive posture a real threat [79]in old Soviet-style.

The Revolution in Military Affairs (RAM) concerning Russia is all about technology and the vision of the future as no-contact and "control war", meant as the extension of the military battlefield to all the aspects of society through "economic coercion, political subversion and the manipulative employment of "information dominance" to weaken and demoralize and adversary (…)"[80], together with disinformation and information manipulation, guerrilla, subversion tactics, were all already elements present in the Soviet warfare style.

In fact, "hybrid warfare as demonstrated in Ukraine consists of no more than conventional warfare coupled with a highly developed disinformation campaign would not indicate anything new in Soviet and Russian practice"[81]. Therefore, it appears that the Russian hybrid warfare model does not respond to an actual Russian doctrine nor strategy, instead "hybrid war' is merely a label attributed to Russian actions in Ukraine by the West, in an effort to make sense of cascading phases of a security crisis in which all sides but Russia seem to have been caught off balance"[82].

[77] Lasconjarias, G., A. Larsen, J. Ibid. p. 58
[78] Giles, K. Op. Cit. p. 9
[79] This position can be supported by the several cases of cyber-attacks in which Russia is somehow implicated, like US hacked election or Brexit case.
D. Kirkpatrick, D. *Signs of Russian Meddling in Brexit Referendum.* https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html and
Swaine, J. *US indicts 12 Russians for hacking DNC emails during the 2016 election.* July 2018. Retrieved from https://www.theguardian.com/us-news/2018/jul/13/russia-indictments-latest-news-hacking-dnc-charges-trump-department-justice-rod-rosenstein
[80] Lasconjarias, G., A. Larsen, J. Ibid. p. 62
[81] Besemeres, J. *Russian disinformation and Western misconceptions*. Inside Story, 23 September 2014. Retrieved from http://insidestory.org.au/russian-disinformation-and-western-misconceptions
[82] Kofman, M., Rojansky, M. *A Closer look at Russia's "Hybrid War".* Wilson Center, April 2015. Retrieved from https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

The creation of a "Gerasimov doctrine[83]", according to which General Valery Gerasimov, Chief of the General Staff of the Russian Federation would have predicted [84]the Russian hybrid warfare used during the Ukraine War, has been made by Western scholars and experts, who looked for a Russian strategy behind the Crime warfare, used as a demonstration of this alleged theory. "The concept of 'hybrid warfare' as a description for the approach pursued by Russia in Crimea does not originate in Russian military strategic thinking. Instead, it was made prominent by Western analysts in the aftermath of the annexation"[85]. And more, a research on Russian language and media coverage for Aleksanteri Papers [86]shown that "when Russian analysts or journalists today speak or write about 'hybrid warfare' ['*gibridnaya voina'*] this is usually in reference to Western discussions of the issue and often in a dismissive way"[87].

The lecture that Western analysts have given of Crimea War "as evidence of a grander master plan of Russian 'hybrid warfare' is reminiscent of the West's enemy image of the Soviet Union"[88], perhaps endangers the great steps that Western countries, and NATO, as a whole, have achieved in the collaboration and partnership in the last decades. Moreover, this Manicheist perspective, confuse and distract from a more efficient and focused analysis of the Russian capabilities and intentions, to work on an effective counterstrategy.

The surprise generated by Russian war tactics and methods in Crimea deals with the "contrast to the Chechen wars and the war with Georgia, which were fought largely as conventional military campaigns relying on heavy and often excessive use of military force"[89]. In fact, it is important to remember that Crimea annexation happened especially thank to a large use of military forces.

It seems that Russia has had a great capacity to learn[90] from those previous armed conflicts, among many other lessons, the fact that the excess of military forces deployment damaged its

---

[83] Gerasimov, V. '*Ценность науки в предвидении'* [*The Value of Science is in Foresight*], *Voyenno-Promyshlennyy Kuryer*. February 2013. Retrieved from http://vpknews.ru/sites/default/files/pdf/VPK_08_476.pdf English translation by Robert Coalson and commentary by Mark Galeotti, https://in-moscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war

[84] K. Bartles, C. *Getting Gerasimov Right*. Military Review.January–February 2016.

[85] Renz, B., Smith, H. *Russia and Hybrid Warfare – Going Beyond the Label*. Aleksanteri Papers. Helsinki. January 2016.

[86] Renz, B., Smith, H. Ibid. p. 8

[87] Renz, B., Smith, H. Ibid. p. 8

[88] Renz, B., Smith, H. Ibid. p. 9

[89] Renz, B., Smith, H. Ibid. p. 10

[90] W. Grau, L., L. Thomas, T. *Russian Lessons Learned From the Battles For Grozny*. Marine Corps Gazette, April 2000. Retrieved from file:///C:/Users/Stefania%20Mascolo/Downloads/2000-04-01%20Russian%20Lessons%20Learned%20From%20the%20Battles%20For%20Grozny%20(Thomas).pdf

capacity to react fast and efficiently. The ability of self-improvement proved by Russia shown its effect in a renovated Russian consciousness and capacity in the Crimea War. However, contextualizing the Russian action, gives a more realistic perspective on its actual capabilities, which fall in between exaggeration of the threat that Russian capabilities can pose to the West, and the underestimation of its strategical and operational development.

In fact, "For countries like Ukraine, hybrid warfare is a tangible threat, but for most European states it poses less of a danger. Such tactics worked so well in parts of eastern Ukraine because it is hard to imagine a more favourable ground: a contested, passive or near-absent sense of Ukrainian identity, estrangement from the new authorities in Kiev, a large-scale Russian military and intelligence presence in Sevastopol, and the domination of Russia-based media outlets. Due to this climate, for it was not just easy for Russia; it was almost effortless."[91]

Beyond the actual novelty of Russian hybrid warfare style in Crimea, what matters is the fact that as state-actor Russia has been able to efficiently deploy and coordinate a mix of conventional and unconventional, previously considered a non-state actors peculiarity. In fact, "the conflict shown the Russian leadership's ability to co-ordinate all relevant instruments of state power, including special operations forces, information operations including state media, elements of cyber warfare, deterrence and coercion through staged military exercises and the use of proxy fighters, for the successful achievement of objective".[92] Including a modernised and efficient Russian military forces, for size, abilities, and resources, included the creation of Special Operation Forces (SOF), as high responsiveness troops.

Russian demonstration of strategical and operational ability is a wake-up call for the West to keep-up with the evolving challenges.

4.2 Terrorist groups: non-state actors hybrid warfare

NATO's engagement in world security is nowadays focused on the Eastern and Southern flanks. A Baltic area threatened by Russian aggressive foreign policy on Eastern Europe, and on the South, the Middle East. As analysed above, Russia represents a peculiar state-actor with the ability to successfully engage hybrid warfare tactics. However, the hybrid warfare was

[91] Popescu, N. *Hybrid warfare: neither new nor only Russian*. European Institute for Security Studies, January 2015. Retrieved from http://www.iss.europa.eu/uploads/media/Alert_4_hybrid_warfare.pdf
[92] Renz, B., Smith, H. Op. Cit. p. 8

traditionally referred to non-state actors, in fact the term was used[93] in 2005 to describe the raising of non-conventional, irregular warfare coming from private group actors, who were developing new threatening tactics to obviate their conventional military force capacity.

Among all the terrorist organizations that in the last decades threatened the global security and represented a powerful adversary and threat in the Middle East and created concern in the West, Hezbollah is a very interesting case of study. "Before Al-Qaeda's attacks on the U.S. in September 2001, Western intelligence services recognised Hezbollah as one of the most dangerous and capable terrorist groups in the world"[94]. As private group, state-backed by Iran, and extensively integrated in the Lebanon parliamentary system, Hezbollah represents the capacity of a non-state actor to not only posing a threat to a sovereign state, but defeating it on the battlefield by using hybrid warfare tactics.

In fact, one year later Hoffman's article, during the 2006 Lebanon War, the Hezbollah group successfully used mixed conventional and unconventional warfare against the Israeli Defence Forces (IDF), which lead to a bitter defeat for a powerful state force: an alarming signal for NATO and Western powers. "Hezbollah clearly demonstrates the ability of nonstate actors to study and deconstruct the vulnerabilities of Western style militaries, and devise appropriate countermeasures[95]".

And more, "Hezbollah affirms an emerging trend. Highly disciplined, well trained, distributed cells can contest modern conventional forces with an admixture of guerrilla tactics and technology in densely packed urban centres"[96].

The rise of irregular hybrid warfare, especially in non-state actor, like terrorist groups, appears to be caused by at least two factors: globalization and the enormous American conventional military strength.

"Our (American) conventional superiority creates a compelling logic for states and non-state actors to move out of the traditional mode of war and seek some niche capability or some unexpected combination of technologies and tactics to gain an advantage. Thus, we need to

[93] Hoffman, F., Mattis, J. N. *Future Warfare: The Rise of Hybrid Wars*. Proceedings. November 2005.
[94] Piotrowski, M., A. *Hezbollah: The Model of a Hybrid Threat.* PISM, The Polish Institute of International Affairs. March 2015.
[95] Hoffman, F. Ibid.
[96] Hoffman, F. *Lessons from Lebanon. Hezbollah and Hybrid Wars*. Foreign Policy Research Institute. August 2006. Retrieved from https://www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/

explore the nature of alternative challenges and the corresponding investments we must make to better posture ourselves for a projected world of more unconventional adversaries."[97]

Moreover, "Irregular warfare is a natural reaction to globalization and America's overwhelming military superiority. Having raised its own way of war to its apotheosis, the United States has turned future opponents to alternative means that are purposely designed and deployed to thwart conventionally oriented Western societies".[98]

NATO's approach to counterterrorism changed after the 9/11 Attacks, embracing international terrorism as a global security threat, requiring a specific set of strategical and operational tools. In the 2010 NATO Strategic Concept[99] terrorism was specifically addressed as a direct threat to the Alliance security. "(…) an "across the board" approach to fighting terrorist networks becomes both sensible and necessary. (…) Defining NATO's own role in countering terrorism becomes a compelling need."[100]

The evolution of the terrorist threat in the last decades involves a more complex and sophisticated, interconnected and trans-national form of terrorism, including: "the established connection between terrorist organizations, insurgent groups, and international organized crime; the emergence of homegrown terrorists and "lone wolves"; reliance on complex funding mechanisms; use of sophisticated propaganda; and access to advanced technologies and fascination with unconventional high-impact operations"[101], while borders become blurred and tactics mixed and unconventional and highly technological.

This is especially true for the Islamic State of Iraq and Syria (ISIS), a terrorist group who grown rapidly in few years, developing a very sophisticated hybrid warfare tactics, based on a well-calibrated and organized blur of several tactics and instruments: from guerrilla, to "highly mobile standoff engagement systems", terrorism, use of cyber propaganda and information warfare, collaboration with other organized crime groups. [102]

---

[97] Hoffman, F., Mattis, J. N. Op. cit.
[98] Hoffman, F. *Complex Irregular Warfare: The Next Revolution in Military Affairs.* Orbis, Summer 2006. p. 397
[99] NATO Strategic Concept – Op. Cit.
[100] Santamato, S., Beumler, M. *The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessments, and Actions*. Institute for National Strategic Studies (INSS) – Strategic Perspective No. 13. Washington DC. February 2013. p. 3
[101] Santamato, S., Beumler, M. p. 3
[102] Jasper, S., Moreland, S. *ISIS: An Adaptive Hybrid Threat in Transition. Small Wars Journals.* 2016. Retrieved from http://smallwarsjournal.com/jrnl/art/isis-an-adaptive-hybrid-threat-in-transition

In particular, information warfare and cyber propaganda, as the most recognizable non-conventional hybrid warfare tools, have been brilliantly mastered by ISIS. "ISIS produced videos depicted ruthless military tactics, brutal mass executions and gory punishments to incite fear, often broadcast on Twitter. (…) During a single summer month, ISIS produced nearly 900 pieces of Arab-language propaganda and nearly half focused on quality of life issues such food, utilities and schools in the attempt to portray a utopian view of life under the caliphate. In the same year, ISIS decided to not just exploit the internet for propaganda purposes but use it as a weapon."

A profitable connection and collaboration among terrorist groups and international crime, like drug-trafficking, from different part of the world, create an intricate network of financial mutual assistance and advantage. "Among the others, these activities and connections give terrorists wider autonomy, making them less dependent on "external" support from sponsor nations, reducing the reach and leverage of any international response".[103]

For NATO, as political-military organization born for well-defined State-against-State type of threats, the current evolving security environment is a real challenge, especially because "the incidence, nature, scope, and, above all, perception of the threat posed by terrorists vary enormously among countries and regions".[104] Based on the concept of collective security, ensured by Article 5, the Alliance needs to recognize a specific common external threat in order to function.

Despite many initiative and programs adopted after 2001, like the "Military Concept for Defence against Terrorism, a Partnership Action Plan against Terrorism (PAP-T), five nuclear, biological, and chemical defence initiatives, protection of civilian populations including a Civil-Emergency Planning Action Plan. (…) The creation of the Defence e Against Terrorism (DAT) Program of Work (POW) to improve the response to new security challenges posed by asymmetric threats. And an Intelligence-sharing was enhanced including through the establishment of a Terrorist Threat Intelligence Unit".[105]

[103] Santamato, S., Beumler, M. p. 5
[104] Santamato, S., Beumler, M. p. 7
[105] Santamato, S., Beumler, M. p. 7

As stated during the Comprehensive Political Guidance at the Riga Summit in November 2006 [106]"terrorism . . . and the spread of weapons of mass destruction are likely to be the principal threats to the Alliance over the next 10 to 15 years".

NATO's activities for counterterrorism focus on share knowledge and capabilities among the Members, with mutual support, but also a stronger collaboration with the United Nations as a forum for International Law[107], legal reference and commitment, and with the European Union, with a new consideration and dialogue with civil society and other local organization.

"Traditional deterrence, based on the threat of retaliation, is not suited for use against non-state groups as they have little to strike back at. There is, however, scope to push back by undermining their support and restricting their actions — including their propaganda, military, terrorist and financial operations."[108]

Moreover, "Non-state actors such as terrorist groups generally do not have targetable assets, and for a non-state actor to tolerate the status quo would be to accept defeat. Highly ideological groups do not change their beliefs in response to physical pressure. Furthermore, the terrorist aim is generally to provoke the state into overreaction, so terrorist groups often welcome attacks by states as this strengthens their support. So, deterrence against non-state groups is difficult".[109]

What is clear for NATO about its counterterrorism capacity is the necessity to go beyond the military means, embracing a more multi-dimensional approach, involving new level of the society, that deal with globalization, digital propaganda, Internet and social networks, and structural issues in Western societies that foment social fractures, as one of the causes of modern terrorism.

5. Policy Implications

Resulting from the above analysis is a struggling NATO, but still main reference for the West. NATO identifies the new challenging security environment, new threats and characteristics,

[106] *Comprehensive Political Guidance*. NATO Heads of State and Government. November 2006. The Strategic Context, paragraph 2. Retrieved from www.nato.int/cps/en/natolive/official_texts_56425.htm
[107] Santamato, S., Beumler, M. p. 12-13
[108] *Global Strategies: Hybrid Warfare in the Middle East*. LSE Ideas. February 2017. Retrieved from http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-Hybrid-Warfare-in-the-Middle-East.pdf
[109] *Global Strategies: Hybrid Warfare in the Middle East*. Op. Cit.

but it seems to have difficulties in a rapid effective adaptation, often holding on to a closed-minded military focus, despite some attempt to embrace a more comprehensive approach.

From a conceptual point of view, NATO's strategy as defined in the 2010 Strategic Concept identifies major threats to the Alliance as traditional-military, as mass destruction weapon, while addressing new non-only military threats as terrorism, transnational organized crime, climate change. However, as this kind of threats fall out of the Article 5 collective defence rule, it seems much harder for the Alliance to effectively engage action. Political decision on the proposed Comprehensive Approach, which would lead the Alliance to a more multi-level and multi-dimensional organization, has revealed the major problem. In fact, at political level, different threat perceptions and political interests impede the creation of a clear and solid strategy with a common support.

At the operational level, the Strategic Concept recognizes the necessity to develop new forms of non-military actions, as crisis management and peace-keeping, also with a new stronger dialogue and collaboration with local authorities and civil populations during operations, however the actual capacity to embrace it was weak. The NRF program resized for objectives and financial means, has shown deep fractures inside the Alliance, uncapable to keep a unified effort.

The analysis shows NATO conscious of the rapidly evolving set of threats, trying to keep up with modernity, but afflicted by internal disagreement and often a myopic point of view.

5.1 Recommendations

1. Cooperation is a good deterrent. Partnerships and cooperation with the EU and UN have already been mentioned by NATO, however, it implementation should be tighter. A more structured collaboration among the three organization regarding hybrid threats, particularly the ones dealing with technologies, cyber-attacks first, would make a unified response much stronger and effective.
2. Comprehensive Strategy. Conceived but still undeveloped, a comprehensive approach is necessary to reinvent NATO as a multi-dimensional organization,

giving a renovated importance to political and societal aspects, like online propaganda, disinformation, fake news and events manipulations, all elements that are brilliantly used by new opponents.

3. A firm aim is worth thousand weapons. The rise in the military expenditure does not mean a better defence when the objective pursued is unclear or different in the same Alliance. Unity of intents among the Allied about who are the enemies and how to fight them, is the strongest port of departure for any strategy.
4. Research. Implementing research, both technical and strategical, is a crucial factor to acknowledge adversaries' thoughts, strategies and tools. The research should never rest, as today the world evolves rapidly, NATO need to be a step ahead and not waiting for threats to manifest.
5. Forward-looking. Using the same mid-set to face the present makes NATO obsolete, comparing to its enemies. A perspective oriented to the future is the only way to keep NATO's strength.
6. Do not rest on your laurels. Military superiority was earlier a deterrent for all kind of enemies. Hybrid warfare, technology and globalization today allow even small groups to be a threat to the Alliance. It is important to not overestimate military superiority as the only necessary winning card.

6. Conclusions

As a result of the analysis, it appears that the instruments, strategical and operational, that NATO developed and used to adapt to the changing security environment in the last two decades have been sometimes just sketched, like the Comprehensive Strategy, sometimes fragile and overestimated, like the NRF. Furthermore, it results that the lack of common interests and perspectives at the internal level of the Alliance, affected its performance in terms of strategies, resource, and credibility.

Likewise, often NATO's experts and policy-makers are victims of old dichotomic West-against-East visions, as demonstrated by the creation of a phantom Gerasimov Doctrine, which affect negatively NATO's capacity to understand and interact in a multipolar world.

The paper highlights important forward moves that NATO achieved facing the hybrid era, but also provide recommendations to boost NATO's capacity to keep its primary role as global

security keeper, first recovering its unit of intents among the Alliance and then proceeding to reinvent and adapt itself to a new set of threats.

Bibliography

Aaronson, M., Diessen, S., De Kemabon, Y., Long M., B., Miklaucic, M. *NATO Countering the Hybrid Threat*. Washington DC. PRISM- Center for Complex Operations at National Defence University. VOL.2. Sept. 2011.

Apps, P. Ukraine crisis gives NATO, West no good options. Reuters online. March 2014. Retrieved from https://www.reuters.com/article/us-ukraine-crisis-west-analysis-idUSBREA210G420140302

Besemeres, J. *Russian disinformation and Western misconceptions*. Inside Story, 23 September 2014. Retrieved from http://insidestory.org.au/russian-disinformation-and-western-misconceptions

Buzan, Barry. Hansen, Lene. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press, 2009.

Comprehensive Political Guidance. NATO Heads of State and Government. November 2006. The Strategic Context, paragraph 2. Retrieved from www.nato.int/cps/en/natolive/official_texts_56425.htm

Cooley, A. *Whose Rules, Whose Sphere? Russian Governance and Influence in Post-Soviet States*. Carnegie Endowment for International Peace. June 2017. Retrieved from https://carnegieendowment.org/2017/06/30/whose-rules-whose-sphere-russian-governance-and-influence-in-post-soviet-states-pub-71403

Department of Defence. *Joint Operating Environment*. Joint Forces Command, February 2010. p.66

D. Kirkpatrick, D. *Signs of Russian Meddling in Brexit Referendum.* Retrieved from https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html

Fukuyama, F. *The End of History and The Last Man*. New York and London: The Free Press, 1992

Gerasimov, V. *'Ценность науки в предвидении'* [*The Value of Science is in Foresight*], *Voyenno-Promyshlennyy Kuryer*. February 2013. Retrieved from http://vpknews.ru/sites/default/files/pdf/VPK_08_476.pdf English translation by Robert Coalson and commentary by Mark Galeotti, https://in-moscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war

Giles, K. *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power.* Research Paper, Russia and Eurasia Programme. March 2016.

Global Strategies: Hybrid Warfare in the Middle East. LSE Ideas. February 2017. Retrieved from http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-Hybrid-Warfare-in-the-Middle-East.pdf

Gray, C. *Another Bloody Century: Future warfare*. London, Weidenfeld and Nicolson, 2005

Hirst, Q. P. *Another Century of Conflict? War and the International System in the 21st Century.* Birbeck College, London. 2002.

Hoffman, F. *Complex Irregular Warfare: The Next Revolution in Military Affairs.* Orbis, Summer 2006. p. 397

Hoffman, F. *Hybrid Warfare and Challenges*. New York. Joint Forces Quarterly 52, First Quarter 2009.

Hoffman, F. *Lessons from Lebanon. Hezbollah and Hybrid Wars*. Foreign Policy Research Institute. August 2006. Retrieved from https://www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/

Hoffman, F., Mattis, J. N. *Future Warfare: The Rise of Hybrid Wars*. Proceedings. November 2005.

Jasper, S., Moreland, S. *ISIS: An Adaptive Hybrid Threat in Transition. Small Wars Journals.* 2016. Retrieved from http://smallwarsjournal.com/jrnl/art/isis-an-adaptive-hybrid-threat-in-transition

K. Bartles, C. *Getting Gerasimov Right*. Military Review.January–February 2016.

Kitzen, M. *Western Military Culture and Counterstrategy: an Ambiguous Reality*. Netherlands Defence Academy, Department Military Operational Art and Science. 2012.

Kofman, M., Rojansky, M. *A Closer look at Russia's "Hybrid War".* Wilson Center, April 2015. Retrieved from https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

Lasconjarias, G., A. Larsen, J.(eds). A. Ruitz Palmer, D. (author). *Back to the Future? Russia's Hybrid Warfare , Revolutions in Military Affairs, and Cold War Comparisons* as part of Research Paper, *NATO's Response to Hybrid Threats*, NATO Defence College. December 2015. p. 50

Lasconjarias, G. *The NRF from Key Driver of Transformation to a Laboratory of the Connected Forces Initiative.* NATO Research Paper – Research Division, Defence College. Rome. January 2013.

Leslie, F., Brown. *Twenty-Frist Century Warfare will be Hybrid*. US Army College, March 2011, 14

Liang, Qiao. Xiangsui, Wang. *Unrestricted Warfare*. Beijing. PLA Literature and Arts Publishing House. February 1999.

Lindley-French, Julian. *NATO and New Ways of Warfare: Defeating hybrid threats*. NATO NDC Conference Report. Research Division – NATO Defence College. May 2015

Macias, A., W. Schoen, J. *Trump pushes NATO allies to increase spending as US share of funding slows.* CNBC. July 2018. Retrieved from https://www.cnbc.com/2018/07/10/trump-pushes-nato-allies-to-increase-spending-as-us-funding-slows.html

Miklaucic, Michael. *NATO Countering the Hybrid Threat*. NATO Allied Command Transformation. Sept. 2011

Murray, W. Millett, A. *Innovation: Past and Future in Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.

NATO ACT Report - *Military Contribution to Countering Hybrid Threats (MCCHT), 3-4.* August 2010.

NATO – Prague Summit Declaration. November 2001. NATO website. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_19552.htm

NATO- Press Release, Public Diplomacy Division. *Defence Expenditure of NATO Countries (2011-2018).* 10 July 2018. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180709_180710-pr2018-91-en.pdf

NATO- *NATO's Readiness Action Plan*. Fact Sheet. NATO website. July 2016.

NATO – *NATO Response Force.* NATO Website. 16 July 2017. Retrieved from *https://www.nato.int/cps/ua/natohq/topics_49755.htm*

NATO- Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. 2010. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

NATO – Supreme Headquarters Allied Powers Europe. *NATO Response Force / Very High Readiness Joint Task Force.* April 2018. Retrieved from https://shape.nato.int/nato-response-force--very-high-readiness-joint-task-force

NATO – retrieved from https://www.nato.int/cps/ua/natohq/topics_50088.htm

Piotrowski, M., A. *Hezbollah: The Model of a Hybrid Threat.* PISM, The Polish Institute of International Affairs. March 2015.

Popescu, N. *Hybrid warfare: neither new nor only Russian*. European Institute for Security Studies. January 2015. Retrieved from http://www.iss.europa.eu/uploads/media/Alert_4_hybrid_warfare.pdf

Reichborn-Kjennerud, E. Cullen, P. NUPI- Norwegian Institute of International Affairs. Policy Brief*, What is Hybrid warfare. 2016.*

Renz, B., Smith, H. *Russia and Hybrid Warfare – Going Beyond the Label*. Aleksanteri Papers. Helsinki. January 2016.

Ringsmose, J. *Taking Stock of NATO's Response Force*. NATO Research Paper- Research Division, Defence College. Rome. January 2010.

Santamato, S., Beumler, M. *The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessments, and Actions*. Institute for National Strategic Studies (INSS) – Strategic Perspective No. 13. Washington DC. February 2013. p. 3

Shanker, T. Landler, M. *Putin Says U.S. Is Undermining Global Stability***.** The New York Times. February 2007. Retrieved from https://www.nytimes.com/2007/02/11/world/europe/11munich.html

S. Lind. William. *Understanding Fourth Generation War*. Military Review. September – October 2004. http://www.au.af.mil/au/awc/awcgate/milreview/lind.pdf

Swaine, J. *US indicts 12 Russians for hacking DNC emails during the 2016 election.* July 2018. Retrieved from https://www.theguardian.com/us-news/2018/jul/13/russia-indictments-latest-news-hacking-dnc-charges-trump-department-justice-rod-rosenstein

The Finnish Defence Forces Website. *NATO's Partnership for Peace.* Retrieved from https://puolustusvoimat.fi/en/international-activities/natos-partnership-for-peace-programme

Traynor, I. *Russia accused of unleashing cyberwar to disable Estonia.* May 2007. Retrieved from https://www.theguardian.com/world/2007/may/17/topstories3.russia. A crucial antecedent of Russia threatening hybrid capability is represented by massive cyber-attacks in 2007 against Estonia, an alarming event for the West.

Van Puyvelde, D. *Hybrid warfare- Does it even exist?* 2015. NATO Review magazine online. https://www.nato.int/docu/review/2015/also-in-2015/hybrid-modern-future-warfare-russia-ukraine/en/index.htm

Von Clausewitz, C. *On War*. Princeston. 1832

W. Glenn, R. *All Glory Is Fleeting: Insights from the Second Lebanon War.* Santa Monica. 2008. p.73.

W. Grau, L., L. Thomas, T. *Russian Lessons Learned From the Battles For Grozny*. Marine Corps Gazette, April 2000.